

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA**

YAEL CANAAN,

Plaintiff,

vs.

CARNEGIE MELLON UNIVERSITY,

Defendant.

Civil Division

Civil Action No.: 23-02107

The Honorable W. Scott Hardy

STIPULATION AND ORDER REGARDING DISCOVERY PROCEDURE

WHEREAS, Rule 26(f) of the Federal Rules of Civil Procedure states that the Parties must develop a proposed discovery plan that states the Parties' views and proposals on, among other things, "any issues about disclosure, discovery, or preservation of electronically stored information, including the form or forms in which it should be produced," Fed. R. Civ. P. 26(f)(3)(C);

WHEREAS, the Parties mutually seek to reduce the time, expense, and other burdens of discovery of certain electronically stored information ("ESI") and privileged materials, as described further below, and to better define the scope of their obligations with respect to preserving such information and materials;

WHEREAS, the Parties therefore are entering into this Stipulation with the request that the Court enter it as an Order;

NOW THEREFORE, it is hereby STIPULATED and ORDERED:

I. GENERAL PROVISIONS & DEFINITIONS

1. Except as specifically set forth herein, this Stipulation and Order does not alter or affect the applicability of the Federal Rules of Civil Procedure or Local Rules for the United States District Court for the Western District of Pennsylvania.

2. The production specifications set forth in this Stipulation and Order apply to Documents and ESI to be produced in the first instance in the above-captioned litigation. To the extent any Producing Party reproduces Documents or ESI previously produced by any Party or Non-Party during a pre-complaint investigation of the subject matter of this litigation, that Party may reproduce such Documents or ESI in the manner in which it was produced to that Party. No Party is obligated to reformat any such prior production in accordance with the production specifications in this Stipulation and Order. Prior productions are nevertheless subject to the privilege obligations set forth in Section IV of this Stipulation and Order.

3. The terms used in this Stipulation and Order that are also used in the Federal Rules of Civil Procedure have the same meaning that they have under the Federal Rules of Civil Procedure, unless otherwise provided in this Stipulation and Order. Whenever the terms set forth below are used in this Stipulation and Order, the following definitions apply:

(a) “Complaint” means the complaint filed by Plaintiff Yael Canaan on December 13, 2023, or any subsequent and operative complaint, in the above-captioned litigation.

(b) “Custodian” means any individual, department, business unit, or division of a Party or Non-party that has possession, custody, or control of Documents, ESI, or data sources.

(c) “Custodial Data Source” means Documents or ESI kept, used, or maintained by a Custodian, including but not limited to personal computers used for business purposes, work stations, email mailboxes (including all email folders, whether on a workstation, mobile device, email server, or local archive), mobile devices (such as cellphones or tablets),

individual folders on networks, cloud storage systems, social media, and documents from a shared network file (including Google Drives) if the Custodian has access to that file, except that no provision of this Stipulation and Order shall require the preservation or production of Documents or ESI that is not reasonably accessible pursuant to Section II of this Stipulation and Order.

(d) “Deduplication” means the process of removing identical copies of documents during a Producing Party’s review of ESI.

(e) “Documents” and “Electronically Stored Information” have the same definition as set forth in Federal Rule of Civil Procedure 34.

(f) “Native Format” means the file structure of a Document created by the original creating application (in contrast to a static image, which is a representation of ESI produced by converting a native file into a standard image format capable of being viewed and printed on standard computer systems, such as .TIFF or .PDF).

(g) “Non-Party” means any natural person, partnership, corporation, association, or other legal entity not named as a Party in the above-captioned litigation.

(h) “Party” or “Parties” means one or more of the parties in the above-captioned litigation.

(i) “Producing Party” means a Party or Non-Party that produces Documents, ESI, or other information in response to a formal or informal request for production of Documents, ESI, or other information.

(j) “Requesting Party” means a Party that requests, formally or informally, the production of Documents, ESI, or other information.

(k) “Search Term” means a combination of words (including synonyms) and phrases designed to capture potentially relevant ESI, and includes strings of words and phrases joined by proximity and Boolean connectors or other syntax.

II. PRESERVATION

1. Materials To Be Preserved. Each Party will continue its retention practices with regards to all Documents and ESI in compliance with duties to preserve material under the Federal Rules of Evidence and the Federal Rules of Civil Procedure, including Federal Rule of Civil Procedure 37(e). The Parties mutually agree that each Party will modify its retention practices as necessary to ensure the preservation of potentially responsive Documents and ESI.

2. Discovery of Material Not Required to Be Preserved. Any discovery request seeking any of the discovery items listed in the paragraph below must include a statement showing good cause for the discovery of such materials, considering the limitations set forth in Federal Rule of Civil Procedure 26(b)(2)(C).

3. ESI That Is Not Reasonably Accessible. The following categories of ESI are not reasonably accessible in this litigation:

(a) Deleted, slack, fragmented, or other data accessible only by forensics (nothing in this order authorizes the intentional deletion of ESI after the duty arose to preserve such ESI);

(b) Data stored in random access memory (“RAM”), temporary files, or other ephemeral data that are difficult to preserve without disabling the operating system;

(c) Online access data such as temporary or cache files, including internet history, web browser cache and cookie files, wherever located;

(d) Dynamic fields or databases or log files that are not retained in the usual course of business;

(e) Data that is not accessible through the operating system or software installed on a device; and

(f) Server, system, or network logs.

4. The Parties need not preserve for this litigation the categories of ESI listed in the paragraph above, unless on the date that this Stipulation and Order is entered by the Court, either Party has a policy that results in the routine preservation of such ESI, in which case such Party shall continue to preserve such ESI in accordance with its policy.

5. Preservation Does Not Affect Discoverability or Claims of Privilege. By preserving Documents and ESI for the purpose of this litigation, the Parties are not conceding that such material is discoverable, nor are they waiving any claim of privilege.

III. PROPORTIONALITY

1. Proportionality. The Parties agree to use reasonable, good faith, and proportional efforts to identify, preserve, collect, process, analyze, review, and produce relevant ESI. This includes identifying appropriate limits to discovery, including limits on custodians, identification of relevant subject matter, time periods for discovery, and other parameters to limit and guide discovery. It also includes the use of technology to achieve an efficient and effective discovery process.

IV. COLLECTION AND REVIEW

1. Search Methodology. The Parties are permitted to use reasonable search and analysis methods to narrow down the ESI to be reviewed for production in discovery including, but not limited to, search terms, date ranges, custodian lists, structured and conceptual analytics, or machine learning (also known as technology assisted review (“TAR”), continuous active learning (“CAL”), or predictive coding). To the extent such methods are used, the Parties shall be prepared to discuss the reasonableness of such efforts. To the extent a Producing Party uses Search

Terms to search for responsive documents, those Search Terms will be run against all of a Custodian's collected Documents.

2. **Responsiveness.** ESI that is captured by application of any search methods or machine learning technology does not mean that such ESI is necessarily responsive to any discovery request or is otherwise relevant to this litigation or any required disclosure, unless otherwise agreed upon by the Parties in writing. Such determinations shall be made by the Producing Party upon review of the ESI. The use of search terms, in particular, does not preclude the use of other reasonable techniques to further identify responsive or non-responsive ESI including, but not limited to, conceptual analytics and machine learning applications.

3. **Attorney Communications.** The Parties agree that neither Party must preserve or produce in discovery documents sent solely between a Party and its outside counsel.

4. **Filtering.**

(a) Producing Parties must de-NIST electronic files, removing known, traceable software applications in the National Software Reference Library ("NIST List"), available at <https://www.nist.gov/itl/ssd/software-quality-group/nsrl-download>.

(b) If a Producing Party proposes to apply other filters to limit ESI that is collected for processing and review (e.g., filters that identify system files, non-user generated files, or zero-byte files), the Producing Party shall advise the Requesting Party and the Requesting and Producing Parties shall meet and confer regarding such additional proposed filters. If the Parties cannot reach agreement, they shall bring their dispute to the Court for resolution.

5. **Deduplication.**

(a) A Producing Party may deduplicate electronic files during their collection and review of Documents and ESI. Before doing so, the Producing Party will provide the

Requesting Party with a written description of its proposed method for Deduplication, including the metadata fields used to calculate the hash value. The Requesting and Producing Parties shall meet and confer regarding the method for Deduplication, and if they cannot reach agreement, they shall bring their dispute to the Court for resolution.

(b) Once the Requesting and Producing Parties agree to a Deduplication methodology, it cannot be altered during the litigation without written notification to and consent from the Requesting Party or, if the parties cannot reach agreement on the modification, with leave of Court.

(c) A Producing Party will not seek to deduplicate: (1) hard copy documents; (2) “loose” electronic documents (e.g., documents located on a Custodian’s local drive) against versions of the document that are attached to emails; or (3) email attachments in one family against email attachments in another family.

(d) All document family groups (e.g., email attachments and embedded files) must be produced together except as limited by any claim of privilege, and child files should follow parent files sequentially in document control numbering.

(e) Deduplication should occur both vertically within each Custodian and horizontally across Custodians. Deduplication must be done in a way that preserves and produces (1) information on blind copy (bcc) recipients of deduplicated emails; (2) information on other Custodians whose files contain deduplicated Documents; and (3) original file path and, if applicable, the mailbox folder information.

V. PRIVILEGE OBLIGATIONS

1. If a Producing Party determines that it has produced Documents or ESI upon which it wishes to make a claim of privilege, it shall promptly, and no later than five (5) days after making such determination, give all counsel of record notice of the claim of privilege. The notice must

identify each such document, unless the review requires additional time, in which case the Producing Party shall notify counsel of record and shall provide a date by which it will provide the identification. If the Producing Party claims that only a portion of a document is privileged, the Producing Party shall provide, along with the notice of the claim of privilege, a new copy of the document with the allegedly privileged portions redacted. Any Producing Party that complies with this paragraph will be deemed to have taken reasonable steps to rectify disclosures of privileged or protected information or materials.

2. If a Party identifies a document that appears on its face or in light of facts known to the Party to be subject to another Party or Non-Party's claim of privilege, the Party identifying the potential claim of privilege is under a good-faith obligation to notify the Party or Non-Party holding the potential claim of privilege. Such notification will not waive the identifying Party's ability to subsequently challenge any assertion of privilege with respect to the identified document. If the Party or Non-Party holding the potential claim of privilege wishes to assert a claim of privilege, it shall provide notice, in accordance with paragraph above, within five (5) business days of receiving notice from the identifying Party.

3. Upon receiving notice of a claim of privilege on a produced document, the Requesting Party shall, in accordance with Federal Rule of Civil Procedure 26(b)(5)(B), promptly sequester the specified information and any copies it has and shall not use or disclose the information until the claim is resolved. Copies of privileged documents or information that have been stored on electronic media that is not reasonably accessible, such as disaster recovery backup media, are adequately sequestered as long as they are not restored; if such data is restored, the Requesting Party shall take steps to re-sequester the restored information. If the Requesting Party

disclosed the information before being notified, it shall take reasonable steps to prevent further use of such information until the claim is resolved.

4. If a Party wishes to dispute a claim of privilege on a produced document asserted under this Order, such Party shall promptly move the Court for an order compelling disclosure of the information. The Party shall follow the procedures described in Federal Rule 26(b)(5)(B) and shall not assert, as a ground for compelling disclosure, the fact or circumstances of the disclosure. Pending resolution of the motion, the Parties shall not use the challenged information for any other purpose and shall not disclose it to any person other than those required by law to be served with a copy of the sealed motion.

5. The Parties may stipulate to extend the periods specified in the paragraphs above.

6. Nothing in this Stipulation and Order overrides any attorney's ethical responsibilities to refrain from examining or disclosing materials that the attorney knows or reasonably should know to be privileged and to inform the disclosing party that such materials have been produced.

7. The Producing Party wishing to assert a claim of privilege retains the burden, upon challenge pursuant to the paragraph above, of establishing the applicability of the claimed privilege.

8. This Stipulation and Order does not preclude a Party or Non-Party from voluntarily waiving any claims of privilege.

9. Nothing in this Section shall be interpreted inconsistently with the Stipulated Scheduling and Case Management Order.

VI. PRIVILEGE LOG

1. For all documents withheld on the basis of privilege, the Producing Party shall provide to the Requesting Party a privilege log consistent with the Federal Rules of Civil Procedure, and at a minimum shall include the following information:

- (a) A unique number for each entry on the log;
- (b) The date of the document, which for emails should be the sent date of the document and for “loose” documents should be the last-modified or creation date of the document;
- (c) The author of the document, which for emails should be populated with metadata extracted from the “Email From” field and for “loose” documents should be populated with metadata extracted from the “EAuthor” or “LastAuthor” field or, if generic or unknown, the “Custodian” field;
- (d) Recipients of the document, which for emails should be populated with metadata extracted from the “Email To,” “Email CC” and “Email BCC” fields;
- (e) The type of privilege being asserted; and
- (f) A description of why such privilege is being asserted over the document, which should include information sufficient to identify whether document contained attachments over which privilege is also being asserted.

2. The parties shall identify on their logs where counsel is present in a conversation and include a reference to relevant counsel involved in the privilege description field described in 1(f) above.

3. Privilege logs may be produced on a rolling basis. The producing party shall provide the Privilege Log and supplements for each production within thirty (30) days of each given production date.

4. If an email contains both privileged and non-privileged communications, the non-privileged communications must be produced, either by separately producing a copy of the non-privileged communications embedded in the privileged communication, or by producing a copy of the entire communication string with the privileged portions redacted.

5. If an email is produced with redactions, the redactions must not obscure the headers (from, to, subject, sent date) of any embedded emails, unless the identity or contact information of a person is privileged or protected.

VII. PRODUCTION

1. Procedures for Production. The following procedures apply to producing Documents or ESI. Compliance with these procedures constitutes compliance with Federal Rule of Civil Procedure 34(b)(2)(E) for this matter.

(a) TIFF Plus Text Productions. Except as stated otherwise below, ESI being produced by a Producing Party shall be converted to 300 dpi, single-page, black-and-white (no shades of gray) TIFF images using CCITT Group IV compression. Where color images are required by this Stipulation and Order, the images shall be in the form of .JPG images. Each page must be branded with a unique Bates number (or alternative document control number), which must not be an overlay of the image. Unless otherwise agreed by the Parties, the TIFF images must be produced electronically by secure FTP, on optical media, or USB hard drive, accompanied by (1) an image cross reference file in OpticonTM format (.OPT) that associates each Bates number with its corresponding single-page TIFF image file (or JPG image file for color images); (2) a “data load file” (.DAT) containing each of the applicable metadata and bibliographic fields described in Appendix A; (3) a comma delimited control list file (.LST) containing the Bates number and the full path to the extracted text/OCR text as it exists on the delivery media; and (4) Custodian Overlay files. The data load file must contain Concordance® delimited text that will

populate fields in a searchable database environment, containing one line for each document. Nothing in this stipulation requires a Party to manually populate a metadata field in Appendix A (other than globally populated bibliographic fields such as MediaID, VolumeName, Company, Custodian, etc.) if such fields cannot be extracted from a Document.

(b) Load file volumes should be as large as practical but not contain more than 200,000 records each. Each volume directory should contain four (4) subdirectories (each may contain sub-directories with no more than 10,000 files per directory): (1) Doclink to contain linked native files; (2) Fulltext to contain extracted/OCR text files; (3) Images; and (4) Loadfiles to contain the .OPT, .LST, .DAT, and Custodian Overlay files.

(c) Documents produced on paper must be organized by Custodian and maintained in the order in which they appear in the files of the Custodian.

(d) Email.

(1) If a Producing Party redacts any part of an email before producing it, OCR text may be provided in place of extracted text.

(2) Email attachments must be processed and produced as though they were separate documents, and the text load file must include fields in which a Producing Party identifies, for each email, and its attachments the BegAttach and EndAttach of the family range.

(3) All hidden text (e.g. track changes, hidden columns, hidden rows, hidden slides, hidden worksheets, mark-ups, notes) shall be expanded and rendered in the extracted text file. For files that cannot be expanded, linked native files shall be produced in addition to extracted text and images.

(e) Native Files.

(1) For Word, WordPerfect, Google Docs, and PDF files, the text load file must contain the full extracted text from the document, unless the document has been redacted during privilege review, in which case the load file may contain OCR text.

(2) For Word, WordPerfect, Google Docs, and PDF files that contain comments or tracked changes that are not part of the ordinary text, the TIFF images must be generated based on how the document appears when first opened using view settings contained in the file.

(f) Microsoft PowerPoint and other presentation files (“Presentations”) must be processed and produced as full color, half page, JPEG images with one slide per page. Any presenter notes must appear below each slide. Presentations must also be produced in Native Format in the Doclinks folder on the production media. The text load file must contain a field that identifies the file path of the native file corresponding to each Document. If Presentations contain privileged text that must be redacted before production, the Producing Party will image the redacted files and provide OCR text for the files. If a Presentation contains embedded Documents, those Documents must be processed and produced as though they were separate Documents with text load files containing BegAttach and EndAttach as described above.

(g) Microsoft Excel and other data spreadsheet files (“Spreadsheets”) must also be produced in Native Format in the Doclinks folder on the production media using the same process as for producing Presentations. If Spreadsheets contain privileged text that must be redacted before production, a Producing Party will image the redacted spreadsheets showing all non-privileged hidden columns and provide OCR text for the files.

(h) Digital photographs must be produced as full color .JPG image files at their original resolution with Bates numbers branded onto them.

(i) Microsoft OneNote files, and files from programs that offer similar functionality as Microsoft OneNote, may be converted to PDF files prior to processing, review, and production. Producing Parties need not collect or produce an entire OneNote notebook if only certain sections or pages in the notebook are responsive.

(j) With respect to any other kinds of electronic data, including data from databases, CAD drawings, GIS data, videos, etc., a Producing Party must produce in Native Format or initiate a meet-and-confer to determine a reasonably usable form for the production. If the file is not one of the types described above, the Producing Party must provide a placeholder TIFF image that shows the name of the file and has a Bates number. If the Requesting and Producing Parties have not agreed on a production format for the ESI prior to the production, then Rule 34(b)(2)(E)(iii) shall not apply to the production.

2. The Requesting Party has the option, after reviewing a black-and-white TIFF image, to enquire whether the original document contained color and, if so, to request color .JPG images.

3. If good cause exists to request production of specified files, other than those specifically set forth above, in native format, the requesting party may request such production and provide an explanation of the need for native file review, which request shall not unreasonably be denied..

4. Document Families. A Producing Party may withhold small image files or extracted embedded files that are unresponsive or irrelevant, even if other documents in the same document family are responsive. A Producing Party shall not withhold documents on a claim of privilege merely because other documents in the same document family are privileged.

VIII. MISCELLANEOUS PROVISIONS.

1. Motions. Before filing any motion with the Court regarding electronic discovery or evidence, the Parties shall meet and confer in a good faith attempt to resolve such disputes. If a discovery dispute cannot be resolved after the parties have conferred in good faith, then the parties shall abide by the Local Rules and Chambers Procedures for the Judge then-assigned to this matter as applicable to the filing of discovery motions.

2. Costs of Document Production. Unless this Court orders otherwise for good cause shown, each Party and Non-Party shall bear the costs of collecting, processing, reviewing, and producing documents in its custody or control. Notwithstanding the foregoing, nothing herein waives Plaintiff's right to recoup fees and expenses pursuant to 42 U.S.C. § 1988 and Federal Rule 54(d).

3. Effect of Order. The Parties' agreement to this Order is without prejudice to the right of any Party or Non-Party to seek an order from the Court to rescind or amend this Order for good cause shown. Nothing in this Order abridges the rights of any person to seek judicial review or to pursue other appropriate judicial action with respect to any discovery ruling made by the Court in this matter.

4. Integration/Appendices. The following documents are incorporated herein by reference:

(a) “Appendix A” is a table describing the fields to be included in the databases produced by each Party.

SO ORDERED this 25th day of February, 2025,

/s/ W. Scott Hardy
HON. SCOTT W. HARDY
U.S. District Judge

Appendix A

Field Name	Field Description	Field Type	Hard Copy	Email	Other ESI	Calendar Items	IMs, Texts, Chats
DOCID	The unique sequential document control number of the first page of the document. Cannot contain spaces or special characters.	Note Text	✓	✓	✓	✓	✓
ENDDOC	The unique sequential control number of the last page of the document. Cannot contain spaces or special characters.	Note Text	✓	✓	✓	✓	✓
COMPANIES	Globally populated field containing the name of producing party (not the law firm or vendor name). Not pulled from metadata.	Multi-Entry	✓	✓	✓	✓	✓
CUSTODIAN	Name of the individual, or group/department for shared resources, from whose files the document originated. Format: Last, First or ABC Dept. Use consistent naming and formatting across all productions.	Note Text	✓	✓	✓	✓	✓
ALLCUSTODIANS	All custodians who were in possession of a deduplicated document, including the person or group identified in the CUSTODIAN field. Format: Last, First or ABC Dept. Use consistent naming and formatting across all productions.	Multi-Entry	✓	✓	✓	✓	✓
MEDIAID	The unique identifier applied to each physical piece of media delivered (e.g., ABC001).	Note Text	✓	✓	✓	✓	✓
VOLUMENAME	Unique production volume identifier applied (e.g., ABC001-001).	Note Text	✓	✓	✓	✓	✓
BEGATTACH	Used for documents in a family group (e.g. an email with attachments). Populated with the document control number of the parent document. Populated for each child document as well as the parent document.	Note Text	✓	✓	✓	✓	✓
ENDATTACH	Used for documents in a family group (e.g. an email with attachments). Populated with the ENDDOC of the last child record in the family group. Populated for each child document as well as the parent document.	Note Text	✓	✓	✓	✓	✓

Field Name	Field Description	Field Type	Hard Copy	Email	Other ESI	Calendar Items	IMs, Texts, Chats
EPROPERTIES	Indicates record type, privilege, translation and other notations. Include all that apply, only the applicable record type or notation category names should be entered: Record Type: Edoc, Edoc Attachment, Email, Email Attachment, Hard Copy, Calendar, Text Message, Text Attachment, IM, Chat, Chat Attachment, Audio, Video, Voicemail. Other Notations: Placeholder, Translation, Translated. Privilege Notations: Redacted, Privileged, Family Member of Priv Doc.	Multi-Entry	✓	✓	✓	✓	✓
TIMEZONE	The TimeZone in which the custodian is normally located.	Note Text		✓	✓	✓	✓
FOLDERLABEL	Full folder path of email within a mail store when collected, including file name; or full folder path of instant message or text message when collected including file name; or Hard Copy folder/binder title/label. Prepend with Custodian Name (sample: Smith, James-Inbox\Active).	Multi-Entry	✓	✓		✓	✓
FROM	Sender of the Email, Instant Message, Text Message, Chat, or Calendar item.	Note Text		✓		✓	✓
TO	Primary recipients of the Email, Instant Message, Text Message, Chat, or Calendar Item. Separate multiple entries with a semi-colon followed by a space.	Multi-Entry		✓		✓	✓
CC	Copies of the Email, Instant Message, Text Message, Chat or Calendar Item. Separate multiple entries with a semi-colon followed by a space.	Multi-Entry		✓		✓	✓
BCC	Blind Copies of the Email, Instant Message, Text Message, Chat or Calendar Item. Separate multiple entries with a semi-colon followed by a space.	Multi-Entry		✓		✓	✓

Field Name	Field Description	Field Type	Hard Copy	Email	Other ESI	Calendar Items	IMs, Texts, Chats
SUBJECT	Subject line of the Email, Instant Message, Text Message, Chat, calendar item, or Notes item.	Note Text		✓		✓	✓
DATEHC	Date of hard copy documents, if coded. Format: MM/DD/YYYY. Leave time segment blank.	Date	✓				
DATESENT	Date and time the Email, Instant Message, Text Message, Chat or Calendar Item was sent. Format: MM/DD/YYYY HH:MM:SS (use 24 hour times, e.g., 13:32:00 for 1:32 pm); time zone indicators cannot be included).	Date-Time		✓		✓	✓
DATERECEIVED	Date and time the Email, Instant Message, Text Message, Chat or Calendar Item was received. Format: MM/DD/YYYY HH:MM:SS (use 24 hour times, e.g., 13:32:00 for 1:32 pm); time zone indicators cannot be included.	Date-Time		✓		✓	✓
HEADER	The internet header information from each Email.	Note Text		✓		✓	
IMPORTANCE	Indicates priority level set for message.	Note Text		✓		✓	✓
SENSITIVITY	Sensitivity field from Email messages or calendar items.	Note Text		✓		✓	
DATECREATED	Date and time the electronic file was created. Format: MM/DD/YYYY HH:MM:SS (use 24 hour times, e.g., 13:32:00 for 1:32 pm); time zone indicators cannot be included).	Date-Time			✓		✓
DATESAVED	Date and time the electronic file was last modified. Format: MM/DD/YYYY HH:MM:SS (use 24 hour times, e.g., 13:32:00 for 1:32 pm); time zone indicators cannot be included.	Date-Time			✓		✓
EAUTHOR	Author field value pulled from the metadata of a native file.	Note Text			✓		
LASTAUTHOR	Last Saved By field value pulled from metadata of a native file.	Note Text			✓		

Field Name	Field Description	Field Type	Hard Copy	Email	Other ESI	Calendar Items	IMs, Texts, Chats
ESUBJECT	Title or Subject field value pulled from metadata from electronic file.	Note Text			✓		
FILENAME	Original file name of the native file, including file extension.	Note Text		✓	✓	✓	✓
APPLICATION	Application used to create or transmit the original native files, document, message, appointment (e.g., WhatsApp, Excel, Slack, Outlook, Snapchat, Word, Twitter, Gmail, Tango).	Note Text		✓	✓	✓	✓
FILEEXTENSION	File extension of original native file; e.g. XLSX, PDF, DOCX	Max 5 chars		✓	✓	✓	
FILEPATH	Full qualified original path to the native when collected, including original file name. Prepend with recognizable Custodian Name.	Multi-Entry		✓	✓	✓	
DOCLINK	File path location to the current native file location on the delivery medium.	Note Text			✓		
DATESTART	Start date and time of calendar appointments, voice messages, chats, text message conversations. Format: MM/DD/YYYY HH:MM:SS (use 24 hour times, e.g., 13:32:00 for 1:32 pm); time zone indicators cannot be included.	Date-Time				✓	✓
DATEEND	End date and time of calendar appointments, voice messages, chats, text message conversations. Format: MM/DD/YYYY HH:MM:SS (use 24 hour times, e.g., 13:32:00 for 1:32 pm); time zone indicators cannot be included.	Date-Time				✓	✓
ACCOUNT	Unique account ID	Note Text					✓
DURATION	The elapsed time of the audio, video, voice message. Format HH:MM:SS	Note Text			✓		
DIRECTION	Identifies direction of communication or other routing information; Outgoing, Incoming.	Note Text					✓

Field Name	Field Description	Field Type	Hard Copy	Email	Other ESI	Calendar Items	IMs, Texts, Chats
TXT-CHATROOMNAME	Name of chat room used in the communications.	Note Text					✓
TXT-PARTICIPANTS	List of participant names and/or telephone numbers.	Note Text					✓
TXT-BODY	Body of text messages, instant messages, notes, or chats. Do not populate for emails or calendar items.	Note Text					✓
TXT-STATUS	Indicates whether text was Sent or Read on the device.	Note Text					✓
TXT-THREAD-GROUP	Populate with the DOCID of the first text in a conversation or chat.	Note Text					✓
HASHMD5	Document MD5 hash value (used for deduplication or other processing).	Note Text		✓	✓	✓	✓
HASHSHA	Document SHA hash value (used for deduplication or other processing).	Note Text		✓	✓	✓	✓